La protection légale des systèmes techniques

Strowel, Alain; Dusollier, Séverine

Published in:
Propriétés Intellectuelles

Publication date:
2001

Document Version
le PDF de l'éditeur

LA PROTECTION LEGALE DES SYSTEMES TECHNIQUES : ANALYSE DE LA DIRECTIVE 2001/29 SUR LE DROIT D'AUTEUR DANS UNE PERSPECTIVE COMPARATIVE

Séverine Dusollier[*] *et Alain Strowel*[**]

En décembre 1996, la communauté internationale négociait et adoptait au sein de l'Organisation Mondiale de la Propriété Intellectuelle deux Traités majeurs dont l'objectif premier était d'adapter le cadre juridique du droit d'auteur et des droits voisins aux nouvelles technologies.[1] L'article 11 du Traité de l'OMPI sur le droit d'auteur (TDA ou WCT en anglais) demande aux Etats d'adopter une protection juridique

> "*contre la neutralisation des mesures techniques efficaces qui sont mises en œuvre par les auteurs dans le cadre de l'exercice de leurs droits et qui restreignent l'accomplissement d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi*"[2].

Ces dispositions restent assez générales et ne précisent en aucune manière comment la protection doit être organisée,[3] ni quels sont les actes précis qui doivent être prohibés. Entière liberté est laissée aux Etats sur ces points.

On aurait donc pu craindre que les dispositions nationales mettant en œuvre ces dispositions divergent sensiblement. Il s'avère, avec le recul de l'analyse, que la loi américaine de 1998 (*Digital Millenium Copyright Act*) et la directive communautaire 2001 du 22 mai 2001 *sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information* (ci-après la « directive sur le droit d'auteur »)[4]offrent deux exemples très similaires de mise en œuvre. Pour mettre en perspective la disposition de la directive communautaire sur le droit d'auteur (art. 6), nous procéderons à une analyse comparative avec le régime existant aux Etats-Unis, mais aussi avec les lois australienne et japonaise.

---

[*] Chargée de recherche au Centre de recherche informatique et droit, Maître de Conférences aux Facultés universitaires Notre-Dame de la Paix, Namur.

[**] Professeur aux Facultés universitaires Saint-Louis, Bruxelles, et à l'Université de Liège; avocat, Covington & Burling, Bruxelles.

1 J. REINBOTHE, M. MARTIN-PRATT, S. VON LEWINSKI : "The New WIPO Treaties : a First Résumé", *E.I.P.R.* 1997/4, p. 173; A. LUCAS, *Droit d'auteur et numérique*, Droit@Litec, 1998, p. 270 et suiv.

2 Voir aussi la formulation équivalente de l'article 18 du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes, TIEP ou WPPT en anglais.

3 S. DUSOLLIER, "Electrifying the fence: the legal protection of technological measures for protecting copyright", *E.I.P.R.*, 1999/6, p. 285-297.

4 *J.O.C.E.*, 22.6.2001, L 167/10.

présenter.

L'une des questions les plus délicates qui sera abordée en conclusions concerne l'interaction entre la question des limitations au droit d'auteur et la possibilité de faire respecter ces limitations en dépit de la protection juridique des mesures techniques, qui ne peuvent que difficilement tenir compte des délicates exceptions voulues par le législateur. Mais avant de se lancer dans une analyse juridique comparative, il convient de définir ce qu'il faut entendre par mesures techniques et préciser quelles en sont les principaux types.

I.. TYPOLOGIE DES MESURES TECHNIQUES DE PROTECTION

Les technologies susceptibles d'être utilisées par les auteurs et autres titulaires de droit pour protéger leurs œuvres et prestations[5] dans la société de l'information sont extrêmement diverses. Certaines ont été conçues spécifiquement pour répondre à la menace que le numérique apportait au droit d'auteur, d'autres ont été développées pour protéger indifféremment tout type de contenu numérique, qu'il soit soumis au droit d'auteur ou non.

Il est difficile de dresser une liste précise des mesures technologiques existantes ou en cours de développement, de même qu'il est impossible de prédire l'avenir de ces technologies dans le domaine de la protection des œuvres soumises au droit d'auteur.[6]

Pour cette raison, nous avons choisi de présenter et de regrouper les mesures techniques de protection du droit d'auteur et des droits voisins en quatre grandes catégories selon le type de fonction principalement poursuivie par ces dispositifs. On peut ainsi distinguer ;

1. les mesures qui protègent effectivement un acte soumis au droit exclusif de l'auteur ;
2. les systèmes d'accès conditionnel (qui, contrôlant l'accès, ne portent pas sur un acte tombant dans le champ du droit d'auteur) ;
3. les outils de marquage et d'identification ;
4. et les systèmes de gestion électronique des droits.

Dans chaque catégorie, des exemples précis de technologies seront brièvement présentés. Notons que tous ces outils reposent essentiellement sur la cryptographie et la stéganographie qui sont des techniques ancestrales, même si le développement du numérique leur apporte une nouvelle jeunesse.

1. Mesures techniques protégeant les droits des auteurs

---

5 Par la suite, pour des raisons de commodité, nous parlerons uniquement de la protection des droits d'auteur sur les œuvres, sans mentionner nécessairement celle des droits connexes portant sur diverses prestations ou objets.

6 D. GERVAIS, *Gestion Électronique des Droits et Systèmes d'Identificateurs Numériques*, Comité consultatif de l'OMPI sur la gestion du droit d'auteur et des droits connexes dans le cadre des réseaux mondiaux d'information, Première session, Genève, 14 et 15 décembre 1998. Voir également NATIONAL ACADEMY PRESS (ed.), *The digital dilemma. intellectual property in the information age*,National Academy Press, Washington, D.C., 2000 et les dispositifs techniques expliqués en annexe.

Il s'agit des outils techniques qui empêchent l'accomplissement de tout acte ou usage soumis aux droits exclusifs des ayants droit, tels que l'impression, la communication au public, la copie digitale, l'altération de l'œuvre, etc. On parle surtout des systèmes anti-copie dont la fonction principale est d'empêcher l'accomplissement d'une copie de l'œuvre ou de l'objet protégé, soit uniquement digitale, soit toute copie numérique ou analogique. Par exemple, le *dongle*, utilisé principalement dans le secteur du logiciel, consiste généralement en un élément du hardware,[7] une sorte de clé, qui se branche sur le port série (*serial port*) de l'ordinateur. Tout logiciel protégé par ce système se connecte alors à cette clé pour vérifier quelle est l'étendue des droits de l'utilisateur. Le principe des dongles apparaît comme un précurseur de la technologie des cartes à puces ou *smart cards* qui autorisent le stockage d'un plus grand nombre d'informations. En outre, ces cartes à puces peuvent contenir des unités de paiement pré-acquittées. Contrairement aux dongles dont l'utilisation s'est jusqu'ici limitée aux logiciels d'un coût élevé, les cartes à puces seront sans doute plus fréquemment utilisées pour les logiciels, ainsi que pour d'autres œuvres offertes au grand public. Ces deux technologies poursuivent à la fois un but d'accès et de contrôle des utilisations, notamment de la copie.

Le *Serial Copy Management System* est un système principalement utilisé aux États-Unis sur les dispositifs d'enregistrement audio digitaux tels le DAT et les mini-disques. Cette technologie permet à l'appareil de décoder les signaux audio intégrés dans le support et de décoder notamment les données relatives à la protection de celui-ci. Le système autorise la réalisation d'une seule copie digitale à partir de l'original, mais empêche toute copie ultérieure. Un système similaire, le *Content Scrambling System,* basé sur la technique de la cryptographie, a été apposé sur les DVD afin notamment d'en empêcher toute reproduction.

2. Systèmes d'accès

L'un des enjeux majeurs des réseaux numériques est de sécuriser l'accès à l'information et aux contenus protégés, à la fois dans le but de garantir le paiement d'une rémunération et pour protéger les droits d'auteur sur l'œuvre. De nombreux systèmes ont donc été mis au point en vue de garantir et sécuriser l'accès soit à une œuvre, soit à un ensemble d'œuvres, soit à un service offrant notamment des œuvres protégées. Désactiver le mécanisme de contrôle d'accès se réalise soit par paiement, soit lorsque les autres conditions de la licence conclue avec les titulaires de droit auront été remplies. Le dispositif d'accès peut ne contrôler qu'un accès initial et ensuite laisser l'œuvre libre de toute utilisation ou vérifier, à chaque nouvel accès, le respect des conditions. L'accès peut également être facilement différencié selon le type d'utilisateurs, ce qui constitue un grand avantage de ces systèmes. Par exemple, une université peut avoir obtenu un accès contre un prix forfaitaire annuel à une œuvre ou à une collection d'œuvres pour un certain nombre d'étudiants et pour une durée d'une année. Le système vérifiera dans ce cas l'existence de la clé de décryptage sur les ordinateurs de l'université ou l'utilisation du mot de passe convenu contractuellement, voire l'identité de l'étudiant. A l'inverse, la même technologie peut accorder des accès répétés à un particulier en échange d'un paiement renouvelé en fonction de l'utilisation.

---

[7] Il peut également s'agir d'une disquette que l'on insère dans l'ordinateur lorsque l'utilisateur souhaite utiliser le logiciel. Le logiciel ne fonctionnera alors qu'à condition que cette disquette soit en possession de l'utilisateur.

Les technologies remplissant cette fonction sont nombreuses : cryptographie, mots de passe, *set-top-boxes*, *black-boxes*, signatures digitales, enveloppe numérique.[8] Le procédé de cryptographie est bien connu. La loi française sur la réglementation des télécommunications le définit comme "*la transformation à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers* ".[9] Dans le monde numérique le cryptage et décryptage se réalise au moyen d'algorithmes de degré de complexité variable. Les signatures digitales sont une application particulière de la cryptographie réalisée pour certifier et identifier un document.[10] Dans le cadre de la protection du droit d'auteur, cette technologie est principalement utilisée pour sécuriser les transmissions des œuvres sur les réseaux et pour veiller à ce que seules les personnes autorisées aient accès à celles-ci. La fourniture de la clé de décryptage se réalise moyennant paiement du prix ou respect des autres conditions auxquelles est subordonnée l'utilisation de l'œuvre.

L'enveloppe digitale ou container numérique est une application de la cryptographie par laquelle une œuvre est "insérée" dans une enveloppe numérique qui contient les informations relatives à l'œuvre et les conditions d'utilisation de celle-ci. Ce n'est qu'en répondant à ces conditions (telles que paiement d'une rémunération, utilisation d'un mot de passe, etc.) que l'enveloppe s'ouvre et que l'utilisateur peut accéder à l'œuvre.

3. Outils de marquage et de tatouage

De nombreuses techniques sont susceptibles de remplir une fonction d'identification et de marquage des œuvres.[11] Les objectifs de ces techniques sont variés, mais leur finalité principale est de servir de support à l'insertion de données relatives à l'œuvre, qu'il s'agisse du titre de l'œuvre, de l'identité de son créateur et du titulaire de droits, ainsi que des conditions d'utilisation. Cette fonction est directement protégée par l'article 12 du Traité de l'OMPI sur le droit d'auteur (TDA)relatif à la protection de l'information sur le régime des droits (voir encore l'article 19 du TIEP). C'est à l'article 7 que la directive sur le droit d'auteur instaure des obligations relatives à l'information sur le régime des droits. On parle ici surtout du procédé de *watermarking* ou tatouage qui permet d'insérer en filigrane certaines informations dans le code de l'œuvre. Ce marquage est en général invisible et inaudible. Cette inscription est réalisée par la technique de la stéganographie qui peut être définie comme "*l'art et la science de communiquer de manière à masquer l'existence même de la communication"*.[12] Dans le monde analogique, l'utilisation d'encre invisible constitue un exemple de cette science millénaire. Dans un environnement numérique, le *watermarking*

---

8 Les dongles et cartes à puces (voir supra) peuvent également avoir une fonction de contrôle d'accès.

9 Loi 90-1170 du 29 décembre 1990, J.O., 30 décembre 1990, p. 16439.

10 J. HUBIN, Y. POULLET, avec la collaboration de B. LEJEUNE et P. VAN HOUTTE, *La Sécurité informatique*, *entre technique et droit*, Cahier du CRID no 14, Bruxelles, Story-Scientia, 1998.

11 S. DUSOLLIER, "Le droit d'auteur et son empreinte digitale", *Ubiquité*, n° 2, Mai 1999, p. 31-47.

12 R. LEYMONERIE, "Cryptage et Droit d'auteur", *Les Cahiers de la Propriété Intellectuelle*, 1998, Vol. 10, n°2, p. 423; voir également D. GUINIER, "La stéganographie, De l'invisibilité des communications digitales à la protection du patrimoine multimédia", *Expertises*, juin 1998, p. 186-190.

modifie certains bits dits "inutiles"[13] d'une image ou d'un son. A l'aide d'un logiciel approprié, ce code numérique peut être extrait et déchiffré. Le marquage est généralement indélébile et se retrouve, même après une altération ou un découpage de l'œuvre, dans chaque partie de celle-ci.

Cependant, d'autres caractéristiques de ces technologies permettent de protéger plus ou moins directement le droit d'auteur. Tout d'abord, le marquage est dans certains cas parfaitement visible, une "marque" est alors clairement apposée sur la représentation de l'œuvre, de manière quelque peu similaire à l'apposition du terme "SPECIMEN" sur des faux billets de banque ou autres papiers officiels. Cette pratique est assez répandue dans le domaine de la photographie : les agences de photos appliquent leur nom ou leur logo sur un exemplaire d'une photo aux seules fins de promotion et ne communiquent l'image débarrassée de ce marquage que lorsque le paiement de la rémunération prévue a été effectué. Certains musées ont aussi choisi de rendre disponibles en ligne des reproductions de leurs collections, mais frappées du sceau du musée.[14] Le *watermarking* remplit dans ce cas une fonction de protection contre la copie dans la mesure où ce marquage apparent diminue les risques d'utilisation commerciale, et donc de copie non autorisée.

Chaque exemplaire distribué aux utilisateurs peut en outre intégrer un numéro de série numérique et distinct. Dans ce cas, une copie pirate retrouvée sur le marché peut révéler l'exemplaire originel à partir duquel cette contrefaçon a été réalisée. Cet estampillage de chaque image permet ainsi de remonter à la source des copies non autorisées à l'aide d'un fichier reprenant les numéros de série et les coordonnées des utilisateurs qui ont bénéficié d'une licence sur ces images estampillées. Ici la fonction essentielle de la technique de protection est d'apporter des éléments de preuve quant à la contrefaçon. Enfin, une dernière fonction utile du *watermarking* est d'authentifier le contenu marqué, en garantissant que l'œuvre conserve son intégrité.

Ces deux dernières fonctions sont particulièrement essentielles pour les services de certification électronique d'œuvres[15] qui apposent un sceau numérique sur l'œuvre et offrent des services de recherche sur Internet d'images ou de contenus copiés sans l'autorisation du titulaire de droits. A cette fin, ils recourent à des agents électroniques qui parcourent le réseau à la recherche de ces sceaux.

4. Systèmes de gestion électronique

Les outils de gestion électronique couvrent toutes les technologies qui assurent la gestion des droits sur les réseaux en permettant la conclusion de licences d'utilisation *on-line* et en contrôlant l'utilisation des œuvres. D'autres fonctions peuvent également être prises en charge par ces outils : la répartition des droits perçus, la perception des paiements, l'envoi de

---

13 Ces bits sont inutiles en ce sens que les images et les sons comprennent un grand nombre de bits dont la suppression ou la modification n'entraînent aucune conséquence perceptible pour l'auditeur ou le spectateur. Ainsi, pour une oeuvre sonore, la ligne de code numérique permettant le marquage est insérée dans les bitscorrespondant à des fréquences inaudible pour une oreille humaine.

14 Un exemple en est la Bibliothèque du Vatican dont les documents précieux ont été numérisés et mis à la disposition du public *on-line*, toutefois recouverts du sceau du Vatican, ce qui empêche toute forme de réutilisation commerciale.

15 Voir par exemple Info2clear (http://www.Info2clear.com) ou Intertrust.

factures, la réalisation de données de profilage des utilisateurs, etc. A titre d'exemple, les agents électroniques ont récemment fait leur apparition sur le marché.[16] Développés pour accomplir de nombreuses fonctions sur les réseaux, certains d'entre eux sont programmés pour négocier et conclure des contrats électroniques.[17] Cette technologie commence à s'appliquer également au droit d'auteur dans la mesure où de tels *contracting agents* accompagnent la diffusion de contenu protégé sur Internet à la fois pour afficher les termes et conditions des licences d'utilisation et pour recevoir et gérer l'acceptation ou le *clic* des utilisateurs. D'autres agents plus performants gèrent complètement de manière automatisée la distribution et l'utilisation de l'œuvre, notamment en intégrant un système de paiement électronique, en renouvelant les licences d'utilisation, ou en réalisant un compte rendu précis de l'utilisation (quelles œuvres ont-elles été copiées, imprimées, agrandies, téléchargées? combien de fois?), à la fois dans un but de facturation adéquate et proportionnelle à l'utilisation réelle et dans un but de marketing ultérieur (quel utilisateur apprécie tel type de musique?). On peut également imaginer que la répartition des droits à destination des auteurs, artistes interprètes et autres titulaires de droits puisse être effectuée en ligne par de tels agents. Lorsque ces agents se contentent de contrôler l'utilisation des œuvres et de dresser la fréquence de consultation des œuvres et des sites web, voire d'établir des profils précis des utilisateurs, on parle souvent de *metering systems*.

Enfin, les *Electronic Right Management Systems ou ERMS* sont sans doute les mesures de protection dont on parle le plus, bien qu'il faut se garder d'y voir une technologie spécifique. Les ERMS (dénommés également *ECMS* pour *Electronic Copyright Management Systems*) consistent plutôt en une combinaison de nombreux outils et technologies dans le but d'exercer plusieurs fonctions.[18] Ainsi, un outil de cryptographie bloquant l'accès à l'œuvre peut être associé à un système anti-copie empêchant la reproduction de l'œuvre même par un utilisateur légitime. La technique du *watermarking* (voir supra) et un système de licence et de paiement électroniques peuvent également être intégrés dans le même programme informatique. Généralement, la fonction principale des ERMS est de gérer les utilisations et licences des œuvres *on-line*. C'est à ce titre que nous les rangeons dans la catégorie des outils de gestion.
De nombreuses sociétés offrent désormais leurs services sur Internet afin de gérer un répertoire ou une collection d'œuvres, de les protéger techniquement et de rechercher et poursuivre les contrefaçons. Nous avons déjà évoqué plus haut (voir fin du point 3) les services de certification électronique qui bien souvent assurent la chaîne complète des opérations liées à la gestion des droits sur Internet.

Outre les quatre fonctions principales des mesures techniques de protection ci-dessus rapidement présentées, d'autres fonctions peuvent être remplies par ces technologies. Elles sont toutefois plus marginales du point de vue du droit d'auteur:

---

16 R. JULIA-BARCELO, "Electronic contracts = A new legal framework for electronic contracts : the EU electronic commerce proposal", *C.L.S.R.*, 06/1999, n° 15/3, pp. 147-158.

17 S. GAUTHRONET ET F. NATHAN, *On-line services and data protection and the protection of privacy*, Étude réalisée pour le compte de la Commission européenne, DG XV, p. 31.

18 M. LEDGER ET J.P. TRIAILLE, "Dispositions contre le contournement des dispositifs techniques de protection", in *Copyright in Cyberspace*, ALAI Study Days, Amsterdam, June 1996, Ed. ALAI, 1997; D. GERVAIS, *Electronic Right Management Systems (ERMS), The next logical step in the evolution of rights management*, (1997), voir http://www.copyright.com/stuff/ecms_network.htm.

– la mention des termes et conditions d'utilisation de l'œuvre;
– la transmission sécurisée du contenu;
– la preuve de la réception du contenu et de l'identité de la personne ayant reçu légitimement ce contenu;
– le paiement;
– l'enregistrement et le suivi des utilisations, notamment dans un but de paiement adéquat ou de marketing.

Ces fonctions sont essentielles au contrôle et à la rémunération des titulaires des droits. Toutefois les technologies qui assurent le bon déroulement de ces autres facettes de la transaction entre un auteur et un utilisateur ne seront pas forcément couvertes par les dispositions légales protégeant les mesures techniques. Il faudra donc trouver une autre base juridique pour poursuivre d'éventuels contrefacteurs de ces systèmes complémentaires. Ce point dépasse le cadre de la présente étude.

II. DISPOSITIFS LÉGAUX DE PROTECTION DES SYSTEMES TECHNIQUES

La technologie dont se servent les auteurs et autres titulaires de droit pour protéger leurs œuvres sert, on vient de le voir, différentes fonctions et est susceptible de sécuriser et de gérer électroniquement une multitude de contenus numériques éventuellement non protégés par un droit intellectuel. Le même système de contrôle d'accès peut être utilisé pour des sites web contenant de la musique, de simples informations financières ou pour la diffusion sur Internet de programmes de télévision. La conséquence en est double.

D'une part, les mesures techniques sont et seront utilisées par différents opérateurs dans des buts très variés. Dès lors, la protection légale de ces techniques peut être consacrée par d'autres textes que ceux relatifs à la propriété intellectuelle.

D'autre part, les systèmes de neutralisation de ces technologies ne vont pas nécessairement porter atteinte à des droits d'auteur, vu que ces technologies pourraient être utilisées pour des contenus non légalement protégés. L'objectif premier de ces dispositifs illicites n'est donc pas forcément de porter atteinte à un contenu protégé par le droit d'auteur ou les droits voisins. Par conséquent, les titulaires de droit pourraient recourir, et il l'ont fait en l'absence de dispositions spécifiques en matière de droit d'auteur, au droit commun qui prévoit des sanctions adéquates en dehors du cadre de la propriété intellectuelle[19].

Nous nous limiterons à examiner les dispositions nationales qui visent à transposer les Traités OMPI de 1996, à l'exception notable de la directive communautaire sur l'accès conditionnel qui occupe une place importante dans les dispositions anti-contournement, quoiqu'elle n'ait aucun rapport direct avec le droit d'auteur.

1. Critères de comparaison des dispositifs légaux

[19] S. DUSOLLIER, "Les protections techniques vues dans un contexte juridique plus large", in *Régimes complémentaires et concurrentiels au droit d'auteur*, Congrès de l'ALAI 2001, New York, 13-17 juin 2001, à paraître, disponible sur <http://www.law.columbia.edu/conferences/2001/home_en.html>.

La complexité des dispositions nationales transposant les Traités OMPI est grande. Il apparaît utile de comparer ces régimes selon les critères suivants :

- **l'objet de la protection et la définition des mesures techniques** : Si le Traité OMPI (art. 11) parle en général des "*mesures techniques efficaces qui sont mises en œuvre par les auteurs dans le cadre de l'exercice de leurs droits"*, les dispositions nationales sont souvent plus précises et limitent la protection en définissant soit les mesures techniques visées, soit le critère d'efficacité qui justifie la protection. Nous verrons également que les législateurs ont souvent institué une protection double à la fois pour les systèmes contrôlant l'accès aux œuvres et pour les systèmes protégeant directement les droits exclusifs de l'auteur (systèmes dits anti-copie : voir supra).

- **l'étendue de la prohibition (acte de neutralisation et/ou actes préparatoires à la neutralisation)** : les textes de l'OMPI semblent ne concerner que l'acte de neutralisation même de la mesure technique de protection. Or, les titulaires de droit et les législateurs insistent sur la nécessité d'une interdiction des activités dites préparatoires à la neutralisation que constituent la fabrication et la mise à la disposition du public de dispositifs de contournement. Il est en effet évident que le préjudice causé aux titulaires de droit sera d'autant plus grand si les moyens techniques de neutralisation sont facilement et largement disponibles sur le marché. Dès lors, la plupart des dispositions ou projets nationaux instituent une double incrimination, d'une part à l'égard des personnes qui neutralisent la mesure technique, d'autre part à l'égard de la commercialisation des dispositifs susceptibles de permettre ou de faciliter cette neutralisation.

- **le type d'activités préparatoires illicites :** les législateurs déterminent généralement strictement les activités susceptibles d'entraîner la responsabilité des fabricants de dispositifs de neutralisation. Dès lors, les activités illicites sont énumérées, de la fabrication à toutes les sortes de distribution au public des dispositifs illicites. Dans ce cadre, nous examinerons si la prestation de services de neutralisation est également incriminée.

- **les conditions d'illicéité des appareils :** une question essentielle est de déterminer à partir de quel moment un dispositif *a priori* licite peut être considéré comme illégitime. Un grand nombre de dispositifs électroniques ou informatiques sont spécifiquement conçus pour contourner la mesure technique et explicitement commercialisés dans ce but. D'autres peuvent être détournés de leur fonction *a priori* légitime afin de servir des objectifs moins licites. Il est donc essentiel de tracer une ligne entre les dispositifs licites et ceux qui ne le sont pas.[21] La définition précise et claire de l'illicéité est d'ailleurs une préoccupation majeure de l'industrie des équipements électroniques qui réclame à cet égard une certaine sécurité juridique. Par exemple, un magnétoscope dont la fonction première est la lecture et l'enregistrement de programmes audiovisuels, mais dont une fonction accessoire permet de neutraliser la protection technique apposée sur les cassettes

---

20 J. REINBOTHE, M. MARTIN-PRATT, S. VON LEWINSKI, op.cit., p. 173.

21 Th. VINJE, "A brave new world of technical protection systems : Will there still be room for copyrigh?", *EIPR,* 1996, n°8, p. 431.

vidéos, est-il illicite? Qu'en est-il d'un logiciel de cryptage que les utilisateurs usent surtout pour décrypter sans autorisation certains signaux? En bref, la fonction de neutralisation doit-elle être principale, unique, prédominante ou simplement accessoire?

- **la connaissance de l'atteinte en tant que condition de la responsabilité :** certains textes exigent de l'auteur des agissements illégitimes une certaine connaissance de l'atteinte au droit d'auteur. Dans certaines législations, l'auteur d'un acte de contournement ne sera responsable que s'il savait ou devait savoir qu'il commet ainsi une infraction au droit d'auteur.

- **le sort des limitations au droit d'auteur :** une des questions les plus controversées en matière de protection légale des mesures techniques est celle du sort réservé aux limitations et exceptions du droit d'auteur et particulièrement la question de savoir s'il est admissible de contourner la protection technique pour exercer un acte non soumis à l'autorisation de l'auteur. Cette question des exceptions présente en réalité deux aspects. D'une part, faut-il tolérer la neutralisation des mesures techniques contrôlant l'accès et l'utilisation d'une œuvre tombée dans le domaine public ou dont l'usage est exempté sur le pied d'une exception légale? D'autre part, doit-on considérer comme illicites la fabrication et la commercialisation de systèmes de neutralisation ne visant qu'à la suppression des technologies apposées sur des éléments du domaine public ou permettant l'exercice d'exceptions?

- **l'existence d'exceptions à l'interdiction de neutralisation :** dans certains cas, la protection légale des systèmes techniques s'accompagne d'une série d'exceptions. Dans ce cas, l'acte de neutralisation et/ou la fabrication et distribution de dispositifs illicites échappent à la prohibition de principe.

- **l'existence d'une clause de *no mandate* :** certains dispositifs techniques exigent une reconnaissance par l'appareil de lecture, de téléchargement ou de reproduction. La protection est dans ce cas intégrée au support ou dans le code numérique de l'œuvre qui envoie un signal à l'appareil pour l'empêcher d'accomplir certaines fonctions (copier l'oeuvre, l'imprimer, y accéder, etc.). L'industrie des équipements électroniques ou informatiques craint d'être tenue d'inclure dans ceux-ci des mécanismes permettant l'interaction avec ces signaux. L'industrie électronique plaide en conséquence pour l'insertion claire dans la loi d'une disposition qui les dispense de conformer leurs produits aux mesures techniques. Une telle disposition est généralement qualifiée de clause de "*no mandate*".

2. Protection des mesures techniques dans l'Union européenne

Avant d'entamer l'analyse des dispositions de la directive du 22 mai 2001 sur le droit d'auteur, il convient de revenir sur un précédent communautaire, contenu dans la directive 91/250/CEE du Conseil concernant la protection juridique des programmes d'ordinateur (ci-après la « directive sur les programmes d'ordinateur » ou la « directive logiciel »).

a) La directive sur la protection des programmes d'ordinateur et sa transposition dans les Etats membres

Le législateur européen s'est pour la première fois penché sur la protection légale des mesures techniques lors de la rédaction de la directive du 19 mai 1991 sur les logiciels. Son article 7 (1) (c) impose aux Etats membres d'incriminer les personnes qui

> "*mettent en circulation ou détiennent à des fins commerciales tout moyen ayant pour seul but de faciliter la suppression non autorisée ou la neutralisation de tout dispositif technique éventuellement mis en place pour protéger un programme d'ordinateur".*[22]

Les mesures techniques ici protégées ne sont pas réellement définies dans le texte européen. Seuls sont visés de manière vague les dispositifs techniques protégeant les programmes d'ordinateur. On pourrait donc considérer que, lorsqu'ils sont appliqués aux logiciels, la plupart des systèmes que nous avons distingués en fonction de leur fonction (voir supra le point A)peuvent rentrer dans cette définition, qu'ils concernent la protection de l'accès ou la copie du programme (contrôle d'accès au logiciel, cryptage du code source, *dongle*, mot de passe, mécanisme de protection contre la copie, etc…). Il en eût été autrement si la disposition avait parlé de mesures techniques protégeant les droits des auteurs sur les logiciels ou utilisées par les auteurs en relation avec l'exercice de leurs droits.

En revanche, l'acte de contournement lui-même n'est pas visé par cette disposition. Seules les activités dites préparatoires, en l'occurrence, dans ce texte, la mise en circulation et la détention à des fins commerciales, sont illicites. La mise en circulation peut se réaliser par la vente, l'offre au public, la location, etc.

Les appareils et systèmes dont la mise en circulation est prohibée sont *tout moyen* dont le *seul but* est de faciliter la suppression ou la neutralisation du dispositif technique. Ce critère est la fois large et assez restreint. D'une part, le terme *"tout moyen",* semble indiquer qu'un large éventail de dispositifs (des logiciels, des éléments d'un système, des appareils, etc.) soient visés. D'autre part, le critère du *"seul but"* réduit largement le champ des dispositifs considérés comme illicites. Par exemple, un logiciel poursuivant un but parfaitement licite mais permettant accessoirement de neutraliser la mesure technique ne sera pas couvert par l'interdiction, même s'il est clair que le succès de ce programme auprès des utilisateurs s'explique par cette fonction accessoire. Ce critère du but unique entraîne par conséquent l'exemption d'un grand nombre de systèmes de la prohibition.[23] Il suffirait de conférer une fonction légitime au dispositif de neutralisation pour pouvoir échapper à l'interdiction. La directive sur les programmes d'ordinateur présente donc une lacune que la Commission elle-même a relevé dans son rapport d'avril 2000 sur la transposition de la directive dans les États Membres[24].

---

22 Directive sur la protection juridique des programmes d'ordinateur du 14 mai 1991, J.O. L 122, 17.5.1991.

23 Th. VINJE, op. cit., p. 431.

24 Rapport de la Commission au Conseil, au Parlement européen et au Comité économique et social sur la mise en œuvre et les effets de la directive 91/250/CEE concernant la protection juridique des programmes d'ordinateur, COM(2000) 199 final du 10.04.2000.

La jurisprudence allemande a toutefois interprété le critère de la directive très généreusement,[25] le seul but de l'application, et non du programme dans son ensemble, ayant été considéré comme suffisant pour interdire la distribution du logiciel permettant la neutralisation. En conséquence, cette interprétation large du texte permettrait de prohiber des mécanismes dont une application a pour seul but le contournement, même si l'équipement en cause poursuit également d'autres objectifs. La terminologie utilisée dans la directive, qui parle de "moyen", autorise cette interprétation.

Pour le reste, les transpositions dans les États membres de cette disposition s'écartent peu du texte de la directive. Par exemple, l'Allemagne a introduit dans sa loi sur le droit d'auteur une disposition interdisant les moyens qui facilitent le retrait ou le contournement non autorisés des mesures techniques protégeant les programmes.[26] La loi belge punit "*ceux qui mettent en circulation ou détiennent à des fins commerciales tout moyen ayant pour seul but de faciliter la suppression non autorisée ou la neutralisation des dispositifs techniques qui protègent le programme*".[27] Estimant que le régime de complicité à la violation du droit d'auteur permettait de poursuivre adéquatement les personnes qui commercialisent des équipements de contournement, le législateur français s'est contenté d'imposer une publicité particulière à ces dispositifs.

La directive européenne sur le droit d'auteur dans la société de l'information, qui sera présentée ci-après, prévoit que la protection juridique qu'elle édicte n'affecte en aucune façon les dispositions spécifiques de la directive sur la protection juridique des programmes d'ordinateur (voir art. 1.2 a)). Autrement dit, l'article 7 de la directive logiciel devra s'appliquer aux mesures techniques utilisées en liaison avec les logiciels. Toutefois, il serait illogique de conserver ce régime qui instaure une protection limitée aux dispositifs dont le seul but est la neutralisation des programmes d'ordinateur, alors que la directive sur le droit d'auteur introduit une protection plus large pour les autres types d'œuvres. Qu'en sera-t-il par exemple de l'acte de contournement d'une mesure technique ? Clairement interdit dans la directive sur le droit d'auteur (voir art. 6.1), cet acte restera-t-il autorisé s'il vise une mesure technique protégeant un logiciel ? Les conséquences de la règle visant à empêcher toute modification de la directive sur les programmes d'ordinateur par la directive sur le droit d'auteur pourraient être étonnantes: imaginons un dispositif de protection consistant à crypter l'œuvre. La même clé sert à crypter des contenus variés, en ce compris des logiciels et des films. La directive sur le droit d'auteur permettrait de poursuivre les personnes qui mettent à disposition du public la clé de décryptage sans poursuivre de fins commerciales, la directive sur les programmes ne le permettant pas. En outre, le régime distinct prévu pour les programmes d'ordinateur pourrait ne pas être conforme aux exigences résultant de l'article 11 du Traité de l'OMPI sur le droit d'auteur qui entend protéger tous types d'œuvres, logiciels y compris.

b) Directive sur le droit d'auteur et les droits voisins dans la société de l'information du 22 mai 2001

---

25 A. RAUBENHEIMER, *Softwareschutz nach den Vorschriften des UWG*, *Computer und Recht*, 1994, p. 264. Voir l'arrêt de la Cour d'appel, de Karlsruhe dans WRP, 1996, p. 587 confirmé par la Cour suprême fédérale (arrêt Bundersgerichtshof in Computer und Recht, 1996, p. 737).

26 Sec. 69 f *Gesetz über Urheberrecht und verwandte Schutzrechte*.

27 Article 10 de la loi belge du 30 juin 1994 transposant en droit belge la directive européenne du 14 mai 1991.

L'article 6 de la directive sur le droit d'auteur est rédigé comme suit :

"1. Les États membres prévoient une protection juridique appropriée contre le contournement non autorisé de toute mesure technique efficace, que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle poursuit cet objectif.

2. Les États membres prévoient une protection juridique appropriée contre la fabrication, l'importation, la distribution, la vente, la location, la publicité en vue de la vente ou de la location, ou la possession à des fins commerciales de dispositifs, produits ou composants ou la prestation de services qui:

a) font l'objet d'une promotion, d'une publicité ou d'une commercialisation, dans le but de contourner la protection ou

b) n'ont qu'une but commercial limité ou une utilisation limitée autre que de contourner la protection ou

c) sont principalement conçus, produits, adaptés ou réalisés en vue de permettre ou de faciliter le contournement de la protection

de toute mesure technique efficace ".

Actes prohibés

Le texte de la directive, après un détour par le Parlement européen, a décidé d'incriminer l'acte de contournement, ainsi que les activités préparatoires. La proposition initiale entretenait un certain flou sur ce point dans la mesure où "toutes les activités" étaient visées. A présent, l'article se subdivise en deux paragraphes distincts, l'un incriminant l'acte de contournement non autorisé, l'autre incriminant les activités notamment de fabrication et de distribution de dispositifs non autorisés.

Le terme de neutralisation qui apparaissait dans les versions antérieures de la directive a finalement été remplacé par celui de contournement, notion bien plus large.

Objet de la protection

Qu'il s'agisse du contournement ou de la distribution de dispositifs le permettant, les mesures techniques protégées sont définies au paragraphe 3 de l'article 6 comme "toute technologie, dispositif ou composant qui, dans le cadre normal de son fonctionnement, est destiné à empêcher ou à limiter les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin (...) ou du droit *sui generis* (...)". Le texte initial de la directive parlait des mesures techniques qui limitaient la violation d'un droit d'auteur ou droit voisin. A première vue, cette définition ne couvrait que les mesures établissant une protection directe des droits de l'auteur, telles que les systèmes anti-copie (voir supra). Désormais, sont non seulement visées les mesures techniques empêchant l'accomplissement d'actes relevant du monopole

légal des auteurs, mais également tout dispositif s'opposant à des utilisations qui ne seraient pas souhaitées par le titulaire de droit. Il suffirait que l'auteur interdise contractuellement une utilisation pour que la mesure technique qui supporte cette interdiction soit protégée par l'article 6 de la directive sur le droit d'auteur.

Toutefois, et suivant en cela les Traités OMPI, les mesures techniques devront être efficaces pour pouvoir bénéficier de la protection. Le législateur européen a introduit une définition de ce critère d'efficacité : "*les mesures techniques sont réputées efficaces lorsque l'utilisation d'une œuvre protégée, ou celle d'un autre objet protégé, est contrôlée grâce à l'application d'un code d'accès ou d'un procédé de protection , tel que le cryptage, le brouillage ou toute autre transformation de l'œuvre ou de l'objet protégé ou d'un mécanisme de contrôle de copie qui atteint cet objectif de protection*."

Cette définition de l'efficacité des mesures techniques appelle plusieurs commentaires. Tout d'abord, le critère de l'efficacité fait référence notamment à l'application d'un code d'accès. Or, l'accès à une œuvre ou à tout autre objet protégé n'est *a priori* pas un acte soumis aux droits exclusifs de l'auteur ou du titulaire de droits voisins.

Le texte initial de la Commission limitait par ailleurs la définition de l'efficacité à l'accès.[29] L'intervention du Parlement européen a ajouté le critère de l'utilisation, ce qui permet de couvrir plus largement les actes accomplis par l'utilisateur, en ce compris les actes de reproduction et de communication au public soumis aux autorisations des titulaires de droit. Depuis l'adoption de la position commune, seul le terme d'utilisation subsiste. Ainsi, si sous l'empire du premier texte, l'on pouvait se demander si les systèmes anti-copie bénéficiaient d'une protection, la nouvelle définition garantit leur protection. La protection finalement instaurée est large puisqu'elle permet d'englober tous les actes effectués par l'utilisateur (allant de l'accès initial à l'œuvre à tous les actes ultérieurs d'utilisation). .

La définition précise en outre que les mesures techniques doivent avoir été appliquées à l'œuvre ou à l'objet protégé avec l'accord des titulaires de droit, qu'ils soient auteurs, artistes-interprètes, producteurs ou exploitants. Toutefois, l'étendue de cette autorisation n'est pas claire et des questions pourraient se poser. L'exploitant qui souhaite sécuriser la distribution des œuvres par un système technique de protection devra-t-il obtenir l'autorisation de tous les titulaires de droit? Imaginons une médiathèque qui souhaite sécuriser les médias qu'elle loue ou prête avec l'autorisation des ayants droit ou la permission de la loi. Devra-t-elle obtenir une autorisation spécifique de chaque titulaire de droit? Si elle ne l'obtient pas, cela signifie-t-il que la poursuite des personnes contournant la protection sera rendue difficile? De manière générale, cette définition des mesures techniques implique-t-elle que seules les technologies employées par les titulaires de droit seront protégées? Le système de la directive sur le droit d'auteur pourrait s'avérer incomplet en ce cas. Mais d'autres textes pourraient apporter une protection à ces systèmes - songeons par exemple à la directive sur l'accès conditionnel bien que cette dernière ne sanctionne pas l'acte de contournement proprement dit.

Enfin, il est précisé que les procédés de protection incluent le cryptage, le brouillage[30] ainsi que « toute autre transformation de l'œuvre ». La référence aux procédés de

---

29 S. DUSOLLIER, "Electrifying the Fence : The legal protection of technological measures for protecting copyright", *E.I.P.R.*, 1999, n° 21/6, p. 285-297.

30 Ce qui montre bien ici que ce texte envisage principalement les systèmes de cryptage et d'accès.

transformation de l'œuvre pourrait couvrir les techniques de *watermarking* ou de tatouage de l'œuvre qui pourtant, ainsi que nous l'avons vu plus haut, ne constituent qu'un mécanisme de protection indirecte de l'œuvre. Ces trois types de procédés ne sont cependant cités qu'à titre d'exemples, ce qui n'exclut pas que des systèmes tels les *dongles* ou d'autres systèmes empêchant la reproduction de l'œuvre soient également visés.

Type d'activités illicites et responsabilité

L'alinéa 1er de l'article 6 inclut l'acte de contournement des mesures techniques dans le champ des activités illicites. Dans ce cas, un élément moral a cependant été ajouté dans le but de ne poursuivre que les personnes qui ont effectué un tel contournement du mécanisme technique en connaissance de cause. La disposition exige que la personne effectuant le contournement le fasse "*en sachant ou en ayant des raisons valables de penser qu'elle] poursuit cet objectif [la neutralisation non autorisée]"*. Il s'agit là d'une condition de connaissance qui n'apparaît pas dans le délit complémentaire lié à l'accomplissement d'actes préparatoires (fabrication, importation, etc. d'appareils de contournement).

Dans le cas des activités préparatoires, le texte européen est très large puisqu'il vise non seulement la fabrication, l'importation, la distribution, la vente, la location, mais aussi la publicité en vue de la vente ou de la location, ainsi que la possession à des fins commerciales et la prestation de services. Toute activité de commercialisation de ces dispositifs non autorisés est donc couverte. De même, les activités non commerciales d'offre de systèmes de contournement semblent également visées. Ainsi, la distribution de clés de décryptage sur Internet, même dans un but non lucratif, à l'instar de ce qui s'est produit pour le décryptage de la protection technique du DVD (voir l'affaire américaine du DeCSS), serait également considérée comme illicite selon la directive communautaire sur le droit d'auteur.

Appareils illicites

L'illicéité des dispositifs et services est quant à elle conditionnée par trois critères alternatifs. Soit le système ou service fait l'objet d'une promotion, d'une publicité ou d'une commercialisation qui évoque l'objectif de contournement de la protection, soit le but commercial ou l'utilisation de tels dispositifs vise principalement à contourner une mesure technique; soit le système ou service est principalement conçu, produit, adapté ou réalisé en vue de permettre ou de faciliter le contournement de la protection.

En quelque sorte, sont visés tous les services et dispositifs qui entendent contourner des mesures techniques, peu importe que cet objectif illicite se révèle dès la conception du système, par la publicité qui se réalise autour de ce produit, par sa principale fonction inhérente ou par l'utilisation postérieure qui en est faite.

La frontière entre systèmes licites et illicites restera soumise à l'appréciation des tribunaux. A titre d'illustrations, le logiciel de cryptage principalement utilisé pour décrypter des œuvres protégées devra être interdit ; de même, un appareil tel qu'un magnétoscope sera à ranger parmi les dispositifs illicites si le vendeur en fait une promotion à des fins de contournement.

Limites du droit d'auteur et protection.

Les systèmes techniques ont pour objet d'empêcher l'accomplissement des actes soumis au droit d'auteur (par ex. des actes de reproduction ou de communication au public de l'œuvre), mais ils ne sont pas à même de déterminer si l'acte bloqué par la protection technique ressort de l'exercice légitime d'une exception. De plus, les mêmes mesures techniques risquent de protéger de manière équivalente les œuvres couvertes par le droit d'auteur et celles tombées dans le domaine public.

C'est la raison pour laquelle la directive sur le droit d'auteur a entendu régler dans un texte particulier (l'alinéa 4 de l'article 6) la question du respect des exceptions en cas d'usage de mesures techniques de protection. On reviendra en conclusions sur cette disposition particulièrement complexe, qui ne résout pas définitivement les problèmes.

Exceptions à l'interdiction de la neutralisation

La question du respect par les mesures techniques des exceptions au droit d'auteur doit être distinguée de la question des exceptions à la protection juridique des mesures techniques. Contrairement à la loi américaine (voir ci-après), la directive sur le droit d'auteur n'énumère pas les exceptions à l'interdiction de principe du contournement. Toutefois, les considérants de la directive nous apprennent que la protection ainsi instaurée ne pourra faire obstacle à la recherche sur la cryptographie,[32] ainsi qu'à la décompilation des logiciels autorisée par la directive sur les programmes d'ordinateur de 1991.[33] Resteront donc permis les actes de neutralisation des mesures techniques pour tester l'efficacité de l'algorithme de cryptage ; de même, l'on ne pourra interdire le contournement d'une protection réalisé afin de décompiler le logiciel. Dans ce dernier cas toutefois, il faudra que la décompilation s'effectue dans les conditions strictes posées par la directive sur la protection des programmes d'ordinateur, notamment le fait que la personne soit un utilisateur légitime du programme et que les informations nécessaires à l'interopérabilité ne soient pas disponibles d'une autre manière. Enfin, cette décompilation ne pourra s'exercer, ainsi que le contournement de la mesure technique effectué à cet effet, que dans le seul but d'assurer l'interopérabilité du programme.

Clause de no mandate

La directive sur le droit d'auteur intègre une clause de *no mandate* (voir supra pour le sens de ce terme) dans ses considérants. Il est ainsi écrit au considérant 48 que la protection ne peut "*empêcher le fonctionnement normal des équipements électroniques et leur développement technique.Une telle protection juridique n'implique aucune obligation de mise en conformité des dispositifs, produits, composants ou services avec ces mesures techniques".* Il n'y a aucune obligation d'intégration pour les fabricants, mais l'objectif de la est toutefois d'encourager les négociations entre les titulaires de droit et l'industrie électronique afin de parvenir à un accord sur l'intégration des mesures techniques dans les équipements électroniques et informatiques.

Il est étonnant de constater la grande convergence entre ce système communautaire de protection et les mécanismes légaux prévus par le législateur américain dans une loi de 1998.

---

32 Considérant 48, *in fine*.

33 Considérant 50.

Mais avant cela, il convient de rappeler succinctement l'apport de la directive communautaire en matière d'accès conditionnel.

c) Directive communautaire protégeant les services à accès conditionnel

Des législations situées hors du champ strict de la propriété intellectuelle apportent dans certains cas une protection aux systèmes techniques qui pourrait notamment être invoquée par les titulaires de droits pour protéger leurs œuvres, particulièrement pour en gérer l'accès.

L'objectif de ces dispositions est généralement de protéger les systèmes techniques empêchant et contrôlant l'accès à certains services. De telles dispositions autrefois prévues pour des services analogiques dans certains pays[34] pourraient être reprises et amplifiées pour le numérique et les services *on-line* en raison de la convergence de l'audiovisuel, de l'informatique et des télécommunications.

Dans le présent cadre, il convient d'examiner une directive européenne qui instaurer une protection supplémentaire des mesures techniques protégeant l'accès à des œuvres protégées. Il s'agit de la directive 98/84/CE du Parlement européen et du Conseil sur la protection juridique des services basés sur ou consistant en un accès conditionnel, directive datée du 20 novembre 1998. Le Conseil de l'Europe a récemment adopté une Convention sur le même thème largement inspirée de la directive communautaire[35].

L'objectif de la directive est de protéger les services dont l'accès est subordonné à certaines conditions, notamment au paiement d'une rémunération, ainsi que de sanctionner la commercialisation de mécanismes facilitant la neutralisation des systèmes d'accès conditionnel. Les services protégés sont notamment la radio et télévision, ainsi que les services de la société de l'information.

Ceci pourrait comprendre les services de vidéo ou d'audio sur demande, l'édition électronique, l'accès à une base de données *on-line*, un site de fichiers musicaux, etc. Par contre, les supports off-line dont l'accès serait régi par un système technique ne seront pas protégés sur base de ce texte, alors que les systèmes techniques appliqués aux produits off-line sont visés par l'article 6 de la directive sur le droit d'auteur.

Les titulaires de droit pourraient donc empêcher la commercialisation de dispositifs permettant le contournement des mesures d'accès auxquelles ils recourent dans le cadre d'un service en ligne qu'ils offriraient. Il convient de préciser dès à présent que cette directive n'a pourtant pas pour objectif de protéger des contenus soumis à la propriété intellectuelle. La proposition initiale excluait d'ailleurs expressément les mesures techniques appliquées aux œuvres protégées par le droit d'auteur. Dans sa version finale, la directive prévoit que son application se fera sans préjudice des dispositions communautaires en matière de propriété intellectuelle dans la directive sur le droit d'auteur dans la société de l'information (voir supra), ce qui ne suffit pas à lever toutes les questions sur le possible double emploi et sur l'articulation des deux textes et l'existence d'une double protection. Les deux directives

---

[34] En matière de cryptage des émissions de télévision, citons les articles 79-1 à 79-6 de la loi française du 30 septembre 1986 relative à la liberté de communication, les articles 297 à 299 de la loi anglaise sur le droit d'auteur, l'article 605 du *Communications Act* aux Etats-Unis.

[35] Convention Européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel, STE n° : 178, 24 janvier 2001.

visent en principe un objet différent : l'objet de la protection sera l'œuvre dans un cas, et un service dans l'autre, qu'il soit composé d'œuvres protégées ou non.

La directive accès conditionnel vise à protéger les services à accès conditionnel ainsi que les technologies qui garantissent et contrôlent cet accès. Dans la mesure où la proposition de directive sur le droit d'auteur définit les mesures techniques comme celles qui contrôlent l'accès aux œuvres, les deux textes sont susceptibles de protéger les mêmes technologies, ainsi que de sanctionner les mêmes types de systèmes pirates. Il faut bien se rendre à l'évidence que la grande majorité des services de la société de l'information comprendront des œuvres protégées par le droit d'auteur ou les droits voisins, ainsi que des bases de données protégées. Une base de données dont l'accès est sécurisé par une mesure technique constituera à la fois une œuvre (ou un objet protégé) et un service à accès conditionnel. La protection sera donc double.[36]

Le critère de la rémunération du service apparaît également comme essentiel à l'application de la directive sur l'accès conditionnel. Toutefois, ceci ne signifie pas que la rémunération doive être antérieure à la fourniture du service, ni être forfaitaire. Ainsi un service à accès conditionnel consistant en une collection on line de photographies, associé à un mécanisme de *metering*, pourrait être protégé, même si la facture comprenant un paiement en fonction de l'utilisation exacte de la photothèque est envoyée à intervalles réguliers après l'accès initial.

La directive sur l'accès conditionnel impose aux États membres d'interdire la fabrication, l'importation, la vente, la distribution, la location, la détention dans un but commercial, l'installation, la maintenance ou le remplacement d'un dispositif permettant l'accès non autorisé à un service protégé, ainsi que la promotion de tels dispositifs ou appareils. Le critère de l'illicéité des dispositifs d'accès non autorisé aux services protégés est plus strict que pour les mesures techniques en matière de droit d'auteur. Seuls les équipements ou logiciels conçus ou adaptés en vue de permettre cet accès seront prohibés.

Évidemment le fait que la protection des services à accès conditionnel soit étrangère aux droits d'auteur et droits voisins empêche que les exceptions et limitations du droit d'auteur puissent être invoquées pour défaire la protection technique. Ainsi, un service d'accès conditionnel comportant des œuvres du domaine public pourrait être protégé par un mécanisme de cryptographie. Les exploitants de ce service pourraient interdire la fabrication de clés de décryptage pirates en invoquant les lois transposant la directive sur l'accès conditionnel. Que les œuvres visées ne fassent plus l'objet d'une protection par le droit d'auteur importerait finalement assez peu (voir encore nos conclusions sur ce sujet).

En conséquence, les titulaires de droit auront parfois intérêt à invoquer ce texte afin d'empêcher la vente de systèmes de neutralisation : les exceptions et limites du droit d'auteur ne pourront lui être opposées. En outre, dans le cadre de la directive accès conditionnel, certaines activités telles que la maintenance, l'installation ou le remplacement d'un tel dispositif sont explicitement sanctionnés, ce que ne prévoit pas la directive sur le droit d'auteur.

---

[36] S. DUSOLLIER *Electrifying the fence* ..., op. cit., p. 290.

3. États-Unis

Avant de présenter les grandes lignes de la loi américaine - il s'agit du *Digital Millenium Copyright Act*-, une révision du *Copyright Act* en 1992 peut utilement être évoquée.

a) Section 1002 du Copyright Act : la protection des Serial Copy Management Systems

Lors des premiers développements d'appareils permettant l'enregistrement et la copie de fichiers audio digitaux, communément appelés *Digital Audio Tape* ou DAT, l'industrie du disque américaine et les titulaires de droit se sont émus que de tels systèmes puissent permettre des copies massives d'œuvres musicales sans aucune perte de qualité et à un moindre coût.

Une modification du *Copyright Act* a alors été adoptée pour imposer l'insertion dans les DAT d'un mécanisme anti-copie empêchant la réalisation de plus d'une copie digitale de l'œuvre (il s'agit des *Serial Copy Management Systems*). En l'espèce, l'industrie a été obligée de conformer sa production aux systèmes techniques alors en cours, et l'on a donc affaire à une disposition qui ne respecte pas la condition de *no mandate*.

Cette modification législative comprend également une interdiction d'importer, fabriquer, distribuer, offrir ou prester un service dont le premier effet ou but est de neutraliser la mesure technique anti-copie.[37] Dans une décisionde 1999,[38] un juge américain a estimé que ces dispositions étaient de stricte interprétation et ne pouvaient par conséquent être étendues à d'autres systèmes que les DAT. L'industrie phonographique essayait de contraindre les fabricants de lecteurs de fichiers MP3, tels la société *Diamond*, à insérer dans leurs appareils un système empêchant la copie des fichiers ainsi que la lecture de fichiers pirates.

b) Digital Millenium Copyright Act

En octobre 1998, le Congrès américain votait le *Digital Millenium Copyright Act*, long texte législatif révisant le *Copyright Act* de 1976. Conçu à la fois pour transposer les traités de l'OMPI et pour réaliser certains points de l'agenda numérique américain,[40] ce texte instaure entre autres un système de protection des mesures techniques.

La section 1201 du *Copyright Act* américain se lit comme suit :

> *(a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES*
>
> *(1) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in*

---

37 Sec. 1002 (c) *: "No person shall import, manufacture, or distribute any device, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent any program or circuit which implements, in whole or in part, a system described in subsection (a)."*

38 *RIAA v. Diamond Multimedia Systems, Inc.*, N° 98-56727 (9th Cir., juin 1999).

40 J. GINSBURG, "Chronique des Etats-Unis", *R.I.D.A*., janvier 1999, p.147 et suiv.

the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.(...)

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that:

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(b) ADDITIONAL VIOLATIONS-

(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

Une double protection est ainsi instaurée : l'une à l'égard des systèmes techniques qui contrôlent l'accès aux œuvres protégées (point a), l'autre à l'égard des mesures techniques qui protègent effectivement un droit exclusif de l'auteur (point b). En réalité, trois infractions sont instaurées par le texte américain : (1) la *neutralisation des mesures techniques* de protection qui *contrôlent l'accès* aux œuvres protégées; (2) *la fabrication et diffusion* de dispositifs ou la *prestation de services* visant à neutraliser les systèmes de *contrôle d'accès*; et, enfin, (3) la *fabrication et diffusion* de dispositifs ou la *prestation de services* permettant la neutralisation de *mesures techniques de protection des droits* des auteurs. Ces trois aspects méritent d'être traités séparément.

i) La protection des systèmes de contrôle d'accès

Objet de la protection

Les mesures technologiques visées sont celles qui "*dans le cadre normal de leur fonctionnement, requièrent l'application d'information, d'un procédé ou d'un traitement, avec l'autorisation des titulaires de droit, afin d'obtenir l'accès à l'œuvre*".[41] Ceci implique certainement les mécanismes de cryptage, d'enveloppe digitale, de dongle, de mots clés.

L'objectif et la fonction principale des technologies dont il est question est de contrôler l'accès à une œuvre, non à un exemplaire ou une copie de l'œuvre.[42] En conséquence, seront protégés par cet article les mécanismes permettant de soumettre à l'autorisation du titulaire de droit, notamment contre paiement renouvelé, chaque nouvel accès ou nouvelle utilisation d'une œuvre sur un support licitement acquis (par exemple, un logiciel sur CD ROM). Dès lors, l'utilisateur ne pourrait, sous peine de sanctions pénales, neutraliser la protection technique attachée à l'œuvre, même s'il a dûment payé en vue d'y avoir accès (une première fois). Cette extension de la protection au-delà des droits traditionnels de l'auteur a déjà suscité des commentaires aux États-Unis.[43]

A titre d'exemple, la jurisprudence américaine a estimé que répondait à la définition de mesures techniques qui contrôlent l'accès à l'œuvre le dispositif de cryptage des DVD. Ce système appelé CSS pour *Content Scrambling System* crypte les films en format DVD qui ne peuvent être visionnés que si le lecteur est muni de la clé de décryptage. Il s'agit bien d 'un mécanisme de contrôle d'accès à l'œuvre puisque seuls les appareils disposant de la clé autoriseront l'accès au film. Dans une autre affaire[44], le juge a considéré qu'une séquence technique d'authentification constituait également une mesure technique de contrôle d'accès. Il était question ici des technologies commercialisées par la firme *RealNetworks* qui permettent de transmettre de la musique ou des œuvres audiovisuelles sur Internet sans en autoriser la copie (transmission sous le format de *streaming)*. De nombreux sites recourent à ce format, notamment pour permettre l'écoute de disques préalablement à leur achat. Les fichiers transmis dans ce format sont hébergés sur des serveurs ou *Realservers* qui ne transmettront les données qu'à un logiciel de lecture *RealPlayer* agréé par *RealNetworks*. Lorsque des données sont demandées par un utilisateur, le *RealServer* vérifie si le demandeur dispose bien du logiciel de lecture adéquat. Ce processus de vérification et d'authentification est la mesure technique principale ; elle est appelée la *Secret Handshake*, soit la *poignée de mains secrète*. Si ce processus échoue, les données ne seront pas transmises. Ce processus consiste donc en une mesure technique de contrôle d'accès selon le juge américain, même si le but de cette poignée de main invisible est avant tout d'assurer que la transmission des données s'effectue vers un logiciel qui respectera les autres conditions techniques d'écoute des fichiers.

---

41 Traduction non officielle de " *if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work"*.

42 J. GINSBURG, op. cit., p. 159.

43 J. LITMAN, *New Copyright Paradigms*, <http://www.msen.com/~litman/paradigm.htm>; D. NIMMER, "Brains and other paraphernalia of the digital age", *Harvard Journal of Law and Technology*, vol. 10, nr. 1, 1996, p. 1-46; J. GINSBURG, op. cit.

44 *RealNetworks v. Streambox*, 2000 WL 141196 * (W.D. Wash. 2000)

Type d'activités illicites

Les dispositions américaines sanctionnent tant la neutralisation de la mesure technique que la fabrication et la commercialisation de dispositifs neutralisant cette protection.

S'agissant de la neutralisation, le texte n'a sorti ses effets que deux ans à dater de l'entrée en vigueur du DMCA. Durant ces deux années, le *Register of Copyright* et le *Librarian of Congress* ont examiné dans quelle mesure cette interdiction du contournement des protections techniques est susceptible de porter préjudice aux utilisateurs d'œuvres protégées, ainsi qu'aux exceptions au droit d'auteur généralement admises au titre du *fair use,* telles que la citation, les usages à des fins d'enseignement, de recherche, le compte rendu d'actualités, etc. L'objectif de ce *rulemaking* est d'exempter certains types d'œuvres de l'interdiction de neutralisation des systèmes d'accès, afin d'en permettre une utilisation légitime (voir ci-après pour un résumé du premier *rulemaking*).

Ce processus d'évaluation de l'effet de la prohibition sera répété tous les trois ans.

L'autre versant de la protection des systèmes d'accès est, quant à elle, entrée en vigueur immédiatement. Elle vise la fabrication, l'importation, l'offre au public, la fourniture ou tout autre type de mise sur le marché de technologies, produits, services, appareils ou éléments illicites. Tant la prestation de services que l'offre de produits sont donc couverts. L'offre de produits sur Internet, comme dans l'affaire du décryptage du DVD que nous avons déjà évoquée plus haut, a été jugée illicite, ainsi que l'établissement d'un hyperlien vers les clés illicites. Parce que l'hyperlien constituait clairement une offre détournée des clés afin d'échapper à une injonction judiciaire, son établissement constituait un acte de mise sur le marché ("trafficking in") répréhensible.

Par contre, aucun élément de connaissance ne vient conditionner la responsabilité ni de la personne qui commet un acte de neutralisation, ni de celle qui fabrique et distribue des dispositifs illicites.

Appareils illicites

Les produits ou services seront jugés illicites lorsqu'ils seront principalement conçus ou fabriqués dans le but de neutraliser une mesure technique, qu'il s'agisse d'un contrôle d'accès ou d'une protection d'un droit exclusif, lorsqu'ils n'ont qu'une raison commerciale ou une utilisation limitée autre que la neutralisation ou lorsqu'ils auront fait l'objet d'une promotion commerciale centrée autour de l'idée de neutralisation. L'application de ces critères n'a jusqu'ici pas posé de difficultés, les équipements mis en cause dans les quelques affaires jugées ayant pour objectif direct de neutraliser le dispositif de cryptage ou de protection. Le fait que le fabricant du mécanisme de contournement soit un commerçant qui développe des produits répondant à un besoin des consommateurs n'a pas pour conséquence d'exonérer la responsabilité de celui-ci . Dans l'affaire *Realnetworks*, la société concurrente *Streambox* plaidait que son magnétoscope remplissait une fonction légitime et comblait une niche dans le marché des équipements électroniques parce qu'il permettait de copier des fichiers transmis en *streaming*. L'argument n'a pas convaincu les juges.

Exceptions à la prohibition de la neutralisation des systèmes d'accès et de la fabrication de dispositifs

Le texte américain ayant fait l'objet d'un intense lobbying de diverses industries et milieux intéressés, de l'industrie informatique et électronique aux bibliothèques, l'interdiction de principe de neutraliser les systèmes techniques de contrôle d'accès connaît certaines exceptions dont le régime est souvent complexe. A cet égard, la loi américaine se distingue sensiblement du cadre juridique de la directive communautaire qui ne propose pas de liste des exceptions, mais suggère simplement que la cryptographie et la décompilation licite constituent des exceptions à l'interdiction de contournement. On se limitera à évoquer ici les principales exceptions de la loi américaine :

- ***exception en faveur des bibliothèques sans but lucratif*** : le §1201 (d) prévoit une exception à l'interdiction de neutralisation au profit non seulement des bibliothèques, mais également au profit des archives et institutions d'éducation qui ne poursuivent pas un but lucratif. Cette exception est limitée à la possibilité de contrevenir à une protection technique dans le seul but de se renseigner sur l'intérêt d'une éventuelle acquisition de l'œuvre protégée. Encore faut-il qu'une copie de cette œuvre ne soit pas autrement disponible et que la bibliothèque se débarrasse de l'exemplaire de l'œuvre à laquelle elle a accédé, une fois sa décision prise. On peut se demander quelle sera l'incidence de cette exception, les éditeurs ayant en effet tout intérêt à fournir un exemplaire aux bibliothèques pour qu'elles puissent déterminer si elles souhaitent en faire l'acquisition. D'autres intérêts de ces institutions, tels que l'archivage ou la préservation, auraient pu être pris en compte.

- ***exception pour les autorités et contrôles de sécurité*** : les autorités officielles ou de police qui contournent les protections techniques dans un but d'investigation ne seront pas soumises à l'interdiction relative aux mesures techniques. Cette exception va de soi, de même que l'exception permettant la vérification de la sécurité d'un système effectuée moyennant l'autorisation du propriétaire de ce système;

- ***décompilation*** : à l'instar de la directive européenne sur la protection des logiciels, le droit américain reconnaît à l'utilisateur légitime d'une copie d'un programme la possibilité de procéder à la décompilation du programme afin d'en assurer l'interopérabilité. Or, les systèmes de contrôle d'accès pourraient anéantir de facto cette possibilité. En conséquence de quoi, la loi prévoit une exception à la criminalisation de la neutralisation de telles mesures techniques. Cette exception est toutefois à interpréter de manière restrictive et raisonnable. La désactivation d'un dispositif technique nécessitera bien souvent une décompilation, qui ne bénéficiera toutefois de l'exception que si elle conduit à l'élaboration d'un programme compatible avec le programme décompilé. L'objectif de la décompilation ne peut être de disséminer le programme de neutralisation ou les informations auxquelles la décompilation a donné accès, tel que par exemple le code de cryptage dans le cas des DVD[45]. En outre, l'exception

[45] Universal City Studios, Inc. v. Reimerdes, 2000 WL 48514 *2 (S.D.N.Y. 2000)

ne profite qu'au décompilateur et non aux personnes qui diffusent l'information décompilée ou l'équipement développé à l'aide du programme décompilé[46];

- ***activités de recherche en matière de cryptographie*** : le § 1201 (g) du DMCA introduit une stricte exception lorsque la neutralisation est nécessaire pour faire avancer la recherche en matière de cryptage, notamment en traquant et vérifiant les points faibles de la technologie. Dans le cadre de cette exception, seule la neutralisation des mesures d'accès est exemptée et non le développement de dispositifs illicites. [47];

- ***exceptions pour les mineurs*** : le législateur américain est très préoccupé par le fait que des mineurs d'âge puissent accéder à des contenus pornographiques ou violents sur Internet. L'industrie a dès lors développé de nombreux systèmes de filtrage, tels que les PICS,[48] pour répondre à ces inquiétudes. Lors des discussions du DMCA, il est apparu que ces systèmes pourraient contenir des composants aptes à neutraliser la protection technique d'accès, précisément pour vérifier la nature du contenu du site visité. Le § 1201 (h) du DMCA prévoit que de tels systèmes ne pourraient être interdits de commercialisation pour ce seul motif;

- ***protection des données à caractère personnel*** : dans la mesure où la technologie d'accès ou le contenu ainsi protégé contient des données personnelles relatives à l'utilisateur – songeons aux *cookies* par exemple – ce dernier est habilité à contourner de telles mesures techniques. L'exception est toutefois limitée à ce seul objectif et ne s'appliquera pas si l'opérateur du système technique informe l'utilisateur de la collecte de données.

Deux exceptions ont été rajoutées à cette liste à l'issue du processus de *rulemaking* effectué par le *Register of Copyright*. Un des moyens offerts par le DMCA pour préserver l'équilibre entre les dispositions anti-contournement et les intérêts des utilisateurs et de la société en général a en effet été de confier au Register of Copyright le soin d'examiner de manière régulière l'incidence de la nouvelle réglementation sur les pratiques des utilisateurs. Dans les deux années qui ont suivi l'adoption du DMCA et par la suite tous les trois ans, la personne accomplissant cette fonction au sein du *Copyright Office*, aura le pouvoir d'exempter de l'interdiction de contournement des mesures techniques d'accès les personnes qui, relativement à des usages légitimes de certaines classes d'œuvres, sont affectées par l'utilisation de ces mesures techniques.

---

46 J. GINSBURG, "Copyright use and excuse on the Internet", 24 *Columbia-VLA J.L. & the Arts*, n°1, 2000, p. 1-45.

47 Cette exception constituera le point le plus intéressant d'une affaire judiciaire introduite aux Etats-Unis à propos du projet d'un professeur (E. Felten) de divulguer les résultats d'une recherche sur les moyens de « craquer » le code du SDMI (Secure Digital Music Initiative).

48 A. LIVORY, "Contrôle du contenu circulant sur Internet : une approche particulière, le contrôle par l'usager et le système PICS", *D.I.T.*, n° 97/2, pp. 52-54; Y. POULLET, *Quelques considérations sur le droit du cyberespace*, FUNDP, Faculté de droit, 1998, 27 p.

Il s'agit là d'une délégation du législateur à une autorité administrative comme l'a clairement qualifié P. Sirinelli[49]. Un processus similaire a été prévu dans la directive européenne sur le droit d'auteur.

Au terme d'une première période de deux ans, le *Register* a rendu ses conclusions qui exemptent deux cas de contournement[50]. Le premier concerne la possibilité de contourner une mesure technique qui bloque l'accès à des "compilations consistant en une liste de sites web faisant l'objet d'un processus technique de filtrage", notamment afin d'empêcher l'accès de mineurs aux sites pornographiques. Afin de dénoncer l'extension des techniques de filtrage à d'autres sites dont l'accès devrait être garanti en vertu de la liberté d'expression, il fallait que le contournement ne soit plus répréhensible et l'on comprend donc aisément pourquoi le *Register* a jugé que cette exception à l'interdiction était légitime.
L'autre exception admise au terme du *rulemaking* a trait aux œuvres littéraires, en ce compris les programmes d'ordinateur et les bases de données, protégées par des mesures techniques qui, par suite d'un mauvais fonctionnement ou d'une obsolescence, bloquent tout accès à l'œuvre. C'est parfois le cas des clés d'accès aux logiciels ou *dongles* développés dans les années 80 et qui dans certains cas ne fonctionnent plus ou ne permettent pas d'assurer l'interopérabilité avec des systèmes informatiques plus modernes. Si le fabricant du *dongle* n'existe plus ou n'accepte pas de remplacer la clé défectueuse, l'utilisateur légitime du logiciel n'aurait pas d'autre choix, selon le *Register*, que le contournement du dispositif d'accès, acte qui devrait, en conséquence, être exempté de l'interdiction du § 1201(a) du DMCA.

Ces deux exceptions demeurent assez ponctuelles..

Limites du droit d'auteur et protection

Le DMCA ne règle pas le statut des actes de contournement effectués pour exercer une exception permise dans le cadre du *fair use,* qui constitue la norme générale du *Copyright Act* à la lumière de laquelle on vérifie si un usage concret peut être exempté. Néanmoins, comme on l'a vu, le législateur a prévu une procédure d'évaluation de l'effet de la prohibition sur les exceptions et limites du copyright (le *rulemaking* dont il a été question ci-dessus). Par ailleurs, l'éventuelle exemption de la protection afin de sauvegarder certaines exceptions ne s'étend qu'aux mesures techniques contrôlant l'accès et non aux mesures de protection des droits exclusifs.

---

49 P. SIRINELLI, « L'étendue de l'interdiction de contournement des dispositifs techniques de protection des droits et les exceptions aux droits d'auteur et droits voisins », in *Régimes complémentaires et concurrentiels au droit d'auteur*, Congrès de l'ALAI 2001, New York, 13-17 juin 2001, à paraître, disponible sur <http://www.law.columbia.edu/conferences/2001/home_en.html>.

50 Library of Congress, *Exemption to prohibition on circumvention of copyright protection systems for access control technologies : Final Rule*, 27 Octobre 2000, Federal Register, Vol. 65, n°209, 64556.

51 Le rapport du Register discute d'ailleurs longuement du sens à donner à cette notion de "certain classes of works" et renvoie la question au législateur. Les autres exceptions invoquées par les parties concernées ont généralement été rejetées parce qu'elles correspondaient à des types d'usages ou d'usagers des œuvres et non à des catégories d'œuvres suffisamment circonscrites. Dans d'autres cas, le Register a jugé que l'incidence des dispositions des DMCA sur l'usage licite n'était à ce stade que virtuelle et qu'aucun exemple d'un effet réel ne pouvait être démontrée.

ii) La protection des mesures techniques protégeant les droits de l'auteur

Objet de la protection

L'alinéa (b) de la section 1201 du DMCA, dont le texte est cité plus haut, vise plus directement à transposer les Traités OMPI dans la mesure où les mesures techniques ici considérées sont bien celles qui protègent les droits reconnus en vertu du droit d'auteur américain, soit les droits de reproduction, d'adaptation, de distribution, de représentation (*public performance)* ou de présentation publique (*public display*) de l'œuvre. Dans ce cadre, la protection instaurée est unique et vise les fabricants et fournisseurs de dispositifs de neutralisation. L'acte de neutralisation lui-même n'est donc pas répréhensible, mais les actes postérieurement accomplis par l'utilisateur constitueront une atteinte au *copyright*. Sans doute a-t-on jugé que dans ce cas la justification d'une sanction supplémentaire ne se justifiait pas.

Les technologies visées sont celles qui protègent efficacement un droit reconnu au titulaire du droit d'auteur . Il s'agit notamment des SCMS et autres dispositifs anti-copie. Les signaux intégrés dans les œuvres en format RealMedia et qui, lorsqu'ils sont reconnus par le logiciel de lecture de l'œuvre, empêchent la copie ont été qualifiés de mesures techniques protégeant les droits des auteurs.

Les actes de commercialisation illicites sont identiques à ceux relatifs aux dispositifs de contrôle d'accès, soit la fabrication, l'importation, l'offre au public, la fourniture ou tout autre type de commercialisation de technologies, produits, services, appareils ou éléments illicites. Il en est de même pour la définition des dispositifs illicites qui s'applique *mutatis mutandis* aux deux types de technologie (d'accès et de protection des droits). Le critère essentiel est également la finalité commerciale ou une utilisation limitée autre que la neutralisation.

Exceptions et mesures techniques de protection des droits

Le contournement n'étant pas interdit en lui-même, les utilisateurs pourront défaire la protection technique pour exercer un acte de *fair use*.

Exceptions à la fabrication de dispositifs illicites

Seule l'exception pour les agissements de l'autorité et des services de police s'applique également dans le cadre des mesures techniques de protection des droits.

Clause de no mandate

---

[52] Dans ce sens, D. NIMMER, "A Riff on Fair Use in the Digital Millenium Copyright Act", 148 U. Pa. L. Rev. 673, 729 (2000).

Le DMCA prévoit que les industries électronique, de télécommunications et informatique ne devront pas adapter leurs produits de manière telle qu'ils puissent interagir avec les mesures techniques de protection ou de contrôle d'accès.[54] Le jugement relatif aux produits développés par *RealNetworks* est particulièrement intéressant à cet égard. Le défendeur, la société *Streambox* avait développé un dispositif qui permettait de copier les fichiers transmis en format de *streaming*. Il estimait ne pas avoir contourné la protection anti-copie consistant en un signal numérique car rien, en vertu de la clause de no-mandate, ne l'obligeait à respecter ce signal. Cette défense a été rejetée car le no mandate ne s'applique que s'il n'y a pas eu de violation des dispositions interdisant le contournement. Or, pour pouvoir ignorer le mécanisme anti-copie, *Streambox* contournait la procédure d'authentification mise en place pour garantir que les œuvres ne soient transmises qu'aux appareils et logiciels respectant ce signal. Jane Ginsburg compare le dispositif anti-copie à une porte ouverte dont la fermeture nécessite un appareil. Le *no mandate* dispense les tiers de conformer leurs équipements afin de permettre la fermeture de la porte. Mais *Streambox* a utilisé une fausse clé pour ouvrir la porte, ce qui lui a permis d'ignorer les instructions de fermeture.

4. Australie : *Copyright amendment Act 2000* (Cth)

L'Australie a transposé les Traités OMPI en 2000[55]. En matière de protection légale des mesures techniques, la loi énonce :

« *A person must not provide a circumvention service if the person knows, or is reckless as to whether, the service will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure.*

A person must not:
(a) make a circumvention device; or

(b) sell, let for hire, or by way of trade offer or expose for sale or hire, a circumvention device; or
(c) distribute a circumvention device with the intention of trading, or engaging in any other activity that will affect prejudicially an owner of copyright; or

(d) by way of trade exhibit a circumvention device in public; or

(e) import a circumvention device into Australia with the intention of:

(i) selling, letting for hire, or by way of trade offering or exposing for sale or hire, the device; or

(ii) distributing the device for trading, or for engaging in any other activity that will affect prejudicially an owner of copyright; or

(iii) exhibiting the device in public by way of trade; or

---

54 Art. 1201 (c) (3).

55 S. FITZPATRICK, «Copyright imbalance: U.S. and Australian responses to the WIPO Digital Copyright Treaty», [2000] *E.I.P.R.* n°5, p. 214-228.

(f) make a circumvention device available online to an extent that will affect prejudicially an owner of copyright;

if the person knows, or is reckless as to whether, the device will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure."

Objet de la protection

Les mesures techniques efficaces qui font l'objet de cette protection sont définies comme *"a device or product, or a component incorporated into a process, that is designed to prevent or inhibit the infringement of copyright subsisting in a work or other subject-matter if, in the ordinary course of its operation access to the work or other subject matter protected by the measure is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) or through a copy control mechanism with the authority of the owner or licensee of the copyright in the work or other subject-matter".*

Dans cette législation également, tant les mesures techniques empêchant la copie de l'œuvre que celles contrôlant son accès sont protégées. L'élément clé de la définition est pourtant l'accès à l'œuvre et non la protection d'un droit spécifique de l'auteur. Contrairement au droit américain, voire au droit européen, aucune protection n'est prévue en parallèle pour les protections techniques empêchant un autre acte d'exploitation que la copie s. Se pose donc la question de l'éventuelle application de ce texte aux technologies qui ne visent ni à contrôler l'accès à l'oeuvre, ni à contrôler sa reproduction[56].

Aucune condition d'effectivité n'est requise pour que les mesures techniques puissent bénéficier de la protection.

Actes prohibés et appareils illicites

Seuls les actes préparatoires à la neutralisation sont sanctionnés et non l'acte de contournement effectué par l'utilisateur. Au titre des actes préparatoires, sont interdits la prestation de service de neutralisation, la fabrication, la vente, la location, l'offre, l'exposition en vue de vente, la commercialisation, la distribution, l'importation ou la mise à disposition *on-line* d'un dispositif de neutralisation.

Toute promotion d'un service ou d'un équipement de contournement est également interdite. La détention d'un équipement de contournement qui serait utilisé pour commettre des violations de droit d'auteur peut également justifier une action du titulaire de droit[57].

---

56 J. DE WERRA, What is a "technological measure" under the WIPO Treaties, the DMCA, the European Union Directives and other legislations (Japan, Australia)?, à paraître dans *R.I.D.A.*, juillet 2001.

57 D. LINDSAY, "The scope of the prohibition on circumvention of technological measures – Rapport australien", in *Régimes complémentaires et concurrentiels au droit d'auteur*, Congrès de l'ALAI 2001, New York, 13-17 juin 2001, à paraître, disponible sur <http://www.law.columbia.edu/conferences/2001/home_en.html>.

Le critère est similaire aux critères européen et américain. Une condition supplémentaire de responsabilité est toutefois prévue dans la mesure où la personne en infraction devra avoir eu la connaissance de l'utilisation de l'appareil ou du dispositif à des fins de contournement.

Limites du droit d'auteur et exceptions

La loi australienne règle d'une manière inédite la délicate question du traitement des exceptions au droit d'auteur. Il est en effet prévu que la prohibition des actes de fabrication et distribution des dispositifs de contournement ou la prestation de service ne s'appliquera pas si la personne à laquelle est fourni ce service ou ce dispositif signe une déclaration selon laquelle elle s'engage à n'utiliser ceux-ci que dans un but permis par la loi, but qui doit également être expressément mentionné sur ladite déclaration. Le but permis par la loi est défini comme l'utilisation de l'appareil ou du service pour accomplir un acte relevant d'une exception au droit d'auteur ou effectué avec l'autorisation du titulaire du droit. Ces exceptions comprennent la décompilation du programme d'ordinateur, la correction de ses erreurs ou les examens de sa sécurité, certains actes de copies licites effectués par les bibliothèques et les institutions éducatives, ainsi que l'usage licite au profit des services de l'autorité publique.

En outre, seules les personnes dites qualifiées peuvent bénéficier de cette dérogation, soit les personnes autorisées à reproduire les œuvres dans le seul cadre des exceptions susmentionnées.

La déclaration doit également préciser que l'œuvre en question n'est pas disponible dans un format non protégé techniquement. L'exception vaut donc seulement pour les œuvres dont la mise sur le marché s'est effectuée exclusivement dans un format techniquement protégé.

Une personne pourrait donc prétendre utiliser un dispositif de neutralisation afin d'effectuer des actes soumis à exception et par là même libérer le fournisseur de toute responsabilité. On peut craindre qu'une telle déclaration ne devienne usage courant dans les contrats de fourniture de tels dispositifs électroniques exonérant pas conséquent les fabricants de leur responsabilité. Toutefois, seules les personnes qualifiées peuvent bénéficier de cette exception–dans le cas des exceptions prévues, ces personnes seront facilement identifiables ; de plus, toute fausse déclaration a été érigée en infraction pénale, ce qui permet de réduire les risques liés à l'adoption de cette règle.

L'approche australienne est intéressante à plusieurs points de vue. Tout d'abord parce que, la loi n'interdisant pas l'acte de contournement lui-même, la question des exceptions ne se posait pas avec la même acuité que dans le contexte européen ou américain. Le législateur aurait pu se contenter de cette absence de prohibition de l'acte. Il va plus loin en offrant aux utilisateurs le bénéfice d'outils de neutralisation lorsque l'exercice d'une exception est en jeu.

Exceptions à l'interdiction de neutralisation

Outre l'exception générale que nous venons d'analyser, la loi prévoit une exception générale à l'interdiction pour les autorités ou services de police.

5. Japon

La transposition japonaise des Traités OMPI présente une particularité remarquable sur le plan de la systématique dans la mesure où un volet de la protection a été introduit dans la loi sur le droit d'auteur et un autre dans la loi sur la concurrence déloyale[59]. Lorsque la mesure technique protège un droit de l'auteur (système anti-copie), l'auteur pourra poursuivre les équipements de contournement sur base des dispositions anti-contournement intégrées dans la loi sur le droit d'auteur. S'agissant des dispositifs de contrôle de l'accès à l'œuvre, les règles prohibant leur contournement ont été insérées dans la loi sur la concurrence déloyale, ce qui s'avère très cohérent pour un système juridique connaissant une loi sur la concurrence déloyale en complément des lois sur la propriété intellectuelle[60].

Objet de la protection

Les mesures techniques protégées par la loi sur le droit d'auteur sont celles qui empêchent ou limitent les actes qui portent atteinte aux droits moraux, aux droits patrimoniaux ou aux droits voisins. Ces mesures doivent avoir été utilisées par les auteurs ou avec leur autorisation et consister en des méthodes d'enregistrement ou de transmission de certains signaux, qui accompagnent la délivrance de l'œuvre et qui enclenchent une réaction des équipements de lecture ou d'utilisation de l'œuvre.

Cette définition recouvre la majorité des techniques actuellement utilisées pour empêcher la reproduction des œuvres. Les mécanismes contre la copie intègrent en effet à l'œuvre des signaux qui donnent ordre au dispositif de lecture ou d'enregistrement de ne pas effectuer de reproduction. Cette définition liée à une technique existante peut toutefois présenter l'inconvénient de ne pas pouvoir s'appliquer aisément à de futurs systèmes techniques qui auraient recours à d'autres méthodes de protection.

La loi sur la concurrence déloyale couvre les moyens qui utilisent une méthode électromagnétique (soit une méthode électronique, magnétique ou autre qui ne peut être perçue humainement) pour restreindre la vision et l'écoute d'images et de sons, l'exécution de programmes ou l'enregistrement d'images, de sons ou de programmes. La technologie utilisée est ici définie plus largement.

Actes prohibés et appareils illicites

Seuls les équipements de neutralisation sont réglementés par la loi japonaise tant en matière de droit d'auteur que dans la loi sur la concurrence déloyale. L'acte de neutralisation n'est en principe pas interdit sauf s'il s'effectue dans un but commercial, ce qui revient en définitive à interdire la prestation d'un service de contournement.

---

59 Amendements du 15 juin 1999 du *Japanese Copyright Law* et du *Japanese Anti-Unfair Competition Law*.

60 TERUO DOI, "WIPO Copyright Treaty and Japanese Copyright Law: A comparative anaysis", *R.I.D.A.*, n°186, Octobre 2000, p.203.

Dans la loi sur le droit d'auteur, des sanctions pénales peuvent être prononcées à l'encontre des personnes qui fabriquent ou mettent en circulation des dispositifs destinés principalement à neutraliser la protection technique. La transmission ou la mise à la disposition du public de logiciels de contournement sont également interdites.

L'illicéité des dispositifs est donc acquise s'ils visent principalement à accomplir une forme de contournement des protections techniques. Ce critère apparaît donc plus strict que celui qui a été adopté par les textes américain, européen et australien.

La loi sur la concurrence déloyale sanctionne la transmission; l'exportation, l'importation, l'offre de dispositifs qui ont comme *seule* fonction d'empêcher les effets d'une mesure technique. Le critère d'illicéité est ici défini de manière encore plus stricte (idée de fonction unique). Toutefois, les équipements incorporant ces dispositifs sont également interdits, ce qui permettrait de sanctionner l'offre de dispositifs dont une des fonctions seulement permet le contournement.

Exceptions et mesures techniques

A notre connaissance, la loi japonaise ne traite pas de la question des exceptions en matière de mesures techniques. C'est compréhensible puisque l'acte de contournement n'est pas interdit, contrairement à ce qui est prévu en Europe et aux Etats-Unis.

III. CONCLUSIONS

Depuis l'adoption des Traités de l'OMPI, quelques pays ont transposé les règles en matière de protection juridique des mesures technologiques ou s'apprêtent du moins à le faire.

Malgré certaines divergences dans l'étendue et les conditions de la protection, les dispositions adoptées en Europe, aux Etats-Unis, en Australie et au Japon s'accordent sur les éléments essentiels d'une protection adéquate, tels que la définition de l'objet de la protection, , et la définition de l'illicéité de ces mécanismes. S'agissant de la délimitation des actes illicites, on remarquera que les Etats-Unis et l'Europe se distinguent de l'Australie et du Japon, en ce que l'acte de neutralisation est également interdit, pas simplement la mise à

---

61 Loi du 15 juin 1999.

62 Proposition pour l'introduction d'un 5ème amendement à la loi allemande sur le droit d'auteur, du 7 juillet 1998, section 96a.

63 En matière de cryptage des émissions de télévision, citons les articles 79-1 à 79-6 de la loi française du 30 septembre 1986 relative à la liberté de communication, les articles 297 à 299 de la loi anglaise sur le droit d'auteur, l'article 605 du *Communications Act* aux Etats-Unis.

64 Convention Européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel, STE n° : 178, 24 janvier 2001.

65 Considérant 15 de la proposition de directive.

66 S. DUSOLLIER *Electrifying the fence* ..., op. cit., p. 290.

67 Article 145 du Code pénal norvégien.

68 *Federal counterfeit access device and computer fraud and abuse Act of 1984*, USC title 18, chapter 47, § 1030.

disposition de mécanismes de contournement. En général, la protection des systèmes techniques est plus étendue dans les textes américain et communautaire.

Au-delà des enseignements de cette approche comparative, il faut souligner qu'unn certain nombre de questions restent ouvertes, la plus délicate étant certainement l'existence d'un possible conflit entre la protection juridique de la mesure technique et les exceptions et limitations aux droits de l'auteur.

a) Les exceptions au droit d'auteur : remises en cause par les mesures techniques?

La question de la préservation des exceptions au droit d'auteur au vu du développement des mesures techniques est au coeur des débats communautaires sur la protection des mesures techniques. La solution communautaire se trouve à l'article 6, 4 de la directive sur le droit d'auteur qui instaure un mécanisme complexe, trop complexe sans doute pour être transposé et mis en oeuvre aisément dans tous les pays de l'Union. Mais il a le mérite d'exister.

La solution consiste à *« encourager les mesures volontaires prises par les titulaires de droits, y compris la conclusion et la mise en oeuvre d'accords entre titulaires de droit et d'autres parties concernées, pour permettre d'atteindre les objectifs visés par certaines exceptions ou limitations prévues par le droit national »* (considérant 51). A défaut de mesures volontaires (*first best solution*), les Etats membres doivent dans certains cas, ou, plus exactement, pour sept exceptions[69], adopter les mesures appropriées pour assurer que les titulaires de droits fournissent aux bénéficiaires des exceptions les moyens d'en bénéficier (par ex., suggère le considérant 51, en modifiant une mesure technique mise en oeuvre). S'agissant de l'exception pour copie privée de l'article 5, 2, b) de la directive, les Etats membres ont la simple faculté d'intervenir *« si, dans un délai raisonnable, aucune mesure volontaire destinée à permettre la reproduction pour usage privé n'a été prise »* (considérant 52).

En d'autres termes, la directive ne résout pas directement la question (une solution radicale, et difficilement défendable, eût été de prévoir des exceptions d'ordre public, comme l'a fait le législateur belge par la loi de 1998), mais s'en remet en premier lieu au marché et aux mesures volontaires adoptées par les parties. Ce n'est que dans un second temps qu'elle oblige ou habilite les Etats membres à intervenir, mais sans trop préciser de quelle manière ou dans quel délai. L'absence d'échéance imposée aux Etats membres a déjà fait l'objet de critiques[70]. L'adoption de ce mécanisme de suivi par les Etats membres montre bien que, pour le législateur communautaire, la question n'est finalement pas mûre[71]. On ne peut lui reprocher

[69] Il s'agit des exceptions pour 1) reprographie, 2) certains actes d'institutions culturelles (bibliothèques, archives, etc.), 3) enregistrements éphémères par les radiodiffuseurs, 4) reproductions d'émissions réalisées par des institutions sociales, 5) usages à des fins d'enseignement ou de recherche, 6) certains usages par les personnes affectées d'un handicap et 7) usages à des fins de sécurité publique ou dans le cadre de procédures.

[70] Th. Vinje, Should We Begin Digging Copyright's Grave?, op. cit., p. 556-557.

[71] Sur ce point, Kamiel Koelman (qui parle de « premature aannames ») rejoint l'analyse des instances communautaires, mais sa solution consiste, au vu des incertitudes subsistantes, à ne pas légiférer du tout, donc à ne pas prévoir de protection légale des mesures techniques. La solution communautaire va de l'avant (protection des mesures techniques, de toute façon imposée par les Traités OMPI de 1996), tout en restant « attentiste » sur le volet de la préservation des exceptions.

de se limiter à mettre en place un mécanisme de veille. On aurait toutefois préféré que ce soit un organisme communautaire qui soit chargé du suivi de la question, à l'instar du *Copyright Office* aux Etats-Unis qui a, comme on l'a vu, procédé à un « rulemaking » en la matière[72]. Cela dit, la Commission s'est réservée la possibilité d'intervenir, puisqu'en vertu de l'article 12 de la directive sur le droit d'auteur, elle est chargée, au plus tard le 22 décembre 2004, et ultérieurement tous les trois ans, de remettre aux autres institutions communautaires un rapport examinant notamment l'application de l'article 6 à la lumière du développement du marché numérique. *« En ce qui concerne l'article 6, elle examine en particulier si cet article confère un niveau suffisant de protection et si des actes permis par la loi sont affectés par l'utilisation de mesures techniques efficaces »*.
La solution communautaire, dont la complexité est certes à critiquer, a donc le mérite de laisser largement la place à un ajustement futur en fonction de l'évolution des marchés, ou en d'autres termes à un mécanisme d'équilibrage entre les intérêts des ayants droit et des usagers. Il est essentiel que l'architecture du droit d'auteur maintienne la possibilité d'un tel ajustement.

b) La protection technique : une possibilité de protéger ce qui ne l'est pas en droit?

Un autre problème résulte de ce que les contrôles d'accès ne peuvent pas aisément tenir compte de ce que les objets ainsi réservés par des techniques d'accès, tout spécialement les bases de données, peuvent contenir des éléments non protégés par le droit.
Imaginons à la suite de J. Ginsburg[73] qu'un ensemble d'éléments du domaine public (décisions de jurisprudence, oeuvres pour lesquelles le délai de protection a expiré, etc.) soit intégré à un produit comprenant des éléments protégés ajoutés à dessein par l'éditeur (une introduction, un résumé original des décisions, etc.). Les mesures techniques de protection, elles-mêmes protégées par le droit, permettraient de bloquer l'accès à des contenus en principe libres.
Soulignons que ce problème spécifique surgit à propos d'une compilation ou base de données, oeuvre qui relève du marché de l'information : s'il ne faut pas aborder la question des mesures techniques uniquement sous l'angle des « produits informationnels », travers qui doit être souligné, en revanche, l'on ne peut laisser de côté les questions tout à fait spécifiques que ce segment du marché pose. La protection des films ou morceaux musicaux (parlons ici de « produits culturels » ou « de divertissement » par opposition aux « produits informationnels ») ne devrait pas, sauf rares exceptions, poser le même problème, puisque le (nouveau) film ou morceaux musical devrait en principe être protégé dans son intégralité. Mais en matière de compilations d'informations et même d'oeuvres, la possibilité de barrer l'accès à des contenus non protégés demeure un vrai problème. On peut se demander s'il ne faudrait pas aborder cette question liée à la protection par des mesures techniques des bases de données.
A cette question particulièrement délicate, la directive n'apporte pas de réponse.

---

[72] Voir US Copyright Office, Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, Recommendation of the Register of Copyrights, 27 oct. 2000 disponible à l'adresse: <http://www.loc.gov/copyright/1201/anticirc.html>

[73] Voir l'article à paraître déjà cité: From Having Copies to Experiencing Works: the Development of an Access Right in US Copyright Law, op. cit.

* *

L'article 6 de la directive communautaire sur l'harmonisation du droit d'auteur et des droits voisins dans la société de l'information est depuis longtemps au centre des débats, et le restera encore lorsqu'il s'agira de transposer la directive en droit interne.
Car, en tout cas, deux questions intéressantes, celle de la préservation des exceptions et celle de l'accès aux éléments non protégés, n'ont pas été pleinement résolues par la directive. Mais appartenait-il au législateur communautaire de régler ces questions aujourd'hui, alors que le marché de la distribution des œuvres en ligne est en train d'évoluer rapidement ?

Août 2001

---

74 J. GINSBURG, op. cit., p. 171.

75 B. HUGENHOLTZ, *Rights, Limitations and Exceptions: Striking a Proper Balance*, Keynote Speech at the Imprimatur Consensus Forum, 30/31 October 1997, Amsterdam; L. GUIBAULT, *Contracts and Copyright Exemptions*, Amsterdam, Institute for Information Law, 1997.